Networked and Layered: Understanding the U.S. Framework for Protecting Personally Identifiable Information[1]

By John W. Kropf[1] *Director of International Privacy Policy for the Department of Homeland Security's Privacy Office*

Following the unprecedented attacks of September 11, the 9/11 Commission recognized the critical role information sharing plays in the fight against terrorism. It issued the following statement, which continues to guide U.S. policy: 'The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation."[2] At the same time, the Commission recognized the need to maintain oversight mechanisms that ensure proper handling of personally identifiable information.

As the U.S. and E.U. look for ways to improve information sharing to fight terrorism and other serious transnational crime,[3] there is particular interest from Europe and privacy advocacy groups in how the U.S. maintains accountability and oversight concerning the use of personally identifiable information. It is not always apparent how oversight works given the many moving parts of the U.S. constitutional form of government.

The European Parliamentary model of government, and its approach to privacy protection, is a clean one: one party or a coalition of parties are in the majority in parliament and run the executive agencies. A single "independent" data protection authority, reporting to parliament and holding the office for a fixed term, regulates both public and commercial flows of personally identifiable information. In contrast, the U.S. model of government, and its approach to privacy protection, is a rich, textured approach; it is layered and networked. This article aims to clarify the U.S. governmental oversight framework with emphasis on law enforcement and home affairs agencies.

I. Accountability and Oversight

Before talking about privacy protection, it is important to understand the structure of U.S. Government. Ours is a system founded on concern, bordering on distrust of government. Accordingly, the Constitution of the United States limits the federal government's powers, spreading them among the three branches at the federal level: the Legislative; Executive and Judicial. Further, the Constitution acknowledges a dual sovereignty within the United States. The duality being that State governments reserve certain powers and rights, even against the federal government. Finally, the Constitution acknowledges the unalienable rights that all persons enjoy, enumerated and unenumerated. The Founders considered this dispersion of power among the people, the states and federal government crucial to good government. This model of checks and balances provides a networked and layered system for accountability and oversight of the federal government's power – including powers affecting privacy.

At the federal level, oversight is achieved through powers exercised by Congress, the executive branch and the judiciary, as set forth in the U.S. Constitution. Within each of these independent,

[1] As published in *World Data Protection Report*, BNA, June 2007

coequal branches exists a variety of oversight bodies that independently review, assess, and report on the actions of federal agencies, including the failures, shortcomings and recommended corrective actions. Each oversight body also has procedures and measures to compel an agency to change policies or systems that are inconsistent with law, policy or otherwise threaten fundamental rights.

With respect to privacy at the federal level, the three core privacy authorities for U.S. Government use of personally identifiable information are: the U.S. Privacy Act of 1974, the Freedom of Information Act (FOIA) and the E-Government Act of 2002. These laws are supplemented with a framework of regulations,[4] Executive Orders[5] and other policies.[6] Other U.S. laws such as the Federal Information Security Act (FISMA) provide for the security of sensitive information that includes protections for personally identifiable information. There are also a number of laws of general application, such as the Whistleblower Act and the Inspector Generals Act of 1978, that provide additional oversight and accountability.

A. Executive Branch: The Network

The executive branch implements law. With respect to privacy, laws are implemented by a network of privacy officials who issue notices, regulations,[7] Executive Orders and Directives.

1. OMB

The starting point in the privacy network is the Office of Management and Budget (OMB), an office within the White House that reports directly to the President. OMB is required under the Privacy Act to prescribe guidelines and regulations for the use of agencies in implementing the Act and to provide continuing assistance to the oversight of the implementation of the Act by agencies. OMB fulfills is its leadership duties by issuing Directives and Memoranda on how best to implement privacy laws among other directives.[8] Related to its privacy mission, OMB also has responsibility to reduce unnecessary burdens on the public through the Paperwork Reduction Act of 1980. The Act requires the OMB Director to develop and implement Federal information policies and standards including policies concerning records management activities and the privacy of records pertaining to individuals. Before a Federal agency may collect information from the public, it must submit to the OMB Director a copy of the proposed rule that specifically describes the proposed information collection request. As part of OMB's oversight, the Director may file public comments on the agency's requests and may direct the agency to publish its responses to such comments with the final rule.

2. Agencies

From its leadership position, OMB extends the privacy network down to Chief Privacy Officers within federal agencies.

a. Chief Privacy Officers

In 1993, the Internal Revenue Service with the Department of the Treasury, created the first full-time privacy position. The U.S. Postal Service followed in 2001. Because of the wide range and volume of personal information collected by these agencies, they were able to pioneer best practices for privacy and develop Privacy Impact Assessments (PIAs).

Then, in 2003, Congress created the first statutorily mandated CPO with the advent of the Department of Homeland Security.[9] The DHS CPO's statutory duties are the following: 1) assure that new technologies do not erode privacy; 2) assure that personal information in Privacy Act Systems of Records is handled in compliance with the FIPs as set out in the Privacy Act; 3) evaluate new legislation on personal information; 4) report to Congress; and 5) coordinate with the DHS Civil Rights and Civil Liberties Office.

Congress reformed the intelligence apparatus in the U.S. Government through the Intelligence Reform and Prevention Act (IRTPA) of 2004, giving intelligence agencies more powers to fight terrorism. Concurrently, it created a Civil Liberties Protection Officer in the Office of the Director of National Intelligence and mandated creation of the Privacy and Civil Liberties Oversight Board.[10] Both of these offices provide oversight on the increased powers given to the intelligence community in the IRPTA. The Board consists of five members appointed by the President with the Chairman and Vice Chairman confirmed by the Senate. The Board advises the President with respect to privacy and civil liberties in the implementation of all laws, regulations and executive branch policies related to efforts to protect against terrorism. In addition, the Board is specifically charged with reviewing the terrorism information sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and civil liberties are being followed. The Board provides advice and recommendations to the President and executive branch department and agency heads, as appropriate, and additionally makes an annual report to Congress.

Given the success of the DHS CPO as an oversight mechanism, Congress further mandated the appointment of a Chief Privacy Officer at the Department of Justice (DOJ)[11] and also separately required that other executive branch departments appoint CPO's.[12] Even though the CPO's position is integral to the agency, such as helping ensure that privacy considerations are integrated into all programs, the CPO also maintains independence from the Department. For example, the CPO is required to prepare an annual report to Congress on departmental activities that affect privacy including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters. In 2005, through OMB Memorandum, OMB required that all federal agencies appoint a senior agency official to assume primary responsibility for privacy policy. This official, usually titled Chief Privacy Officer (CPO), enforces privacy policy and provides guidance tailored to the particular agency, monitors compliance with applicable laws and policies and supports requests for information and redress from the public.

OMB and the CPOs maintain their network through formal interactions such as the approval process for a Privacy Act System of Records Notice (SORN) (discussed below). CPOs also coordinate through informal meetings and conversations to discuss on privacy issues of the day.

b. Rule Making and Funding

Privacy laws ensure transparency in federal agencies' collection and use of personally identifiable information. The Privacy Act of 1974 requires that the individual be provided notice of the agency's use, dissemination and maintenance of the personally identifiable information it collects. There are several administrative processes required by these laws that allow the public

an opportunity to receive and consider notice of an agency's collection or use of personally identifiable information.

For instance, the Privacy Act requires agencies to publish in the Federal Register Systems of Records Notices (SORNs) that specify how an agency maintains personally identifiable information, its purposes for collection and any allowances for the use and disclosure of a record without the prior consent of the individual. Agencies must also notify the public of how an individual may seek access, correction and redress for information contained about the individual in the system of record. The SORN must be submitted to OMB and to Congress for 40 days of review, concurrent with the publication of the SORN in the Federal Register.

Additionally, the Privacy Act allows for the exemption of certain records, such as certain law enforcement records, from certain requirements of the Privacy Act. In order to request an exemption for eligible records, an agency must publish in the Federal Register a Notice of Proposed Rule Making (NPRM) in which the agency explains in detail what particular exemptions are being requested and the specific reasons why. Public comments received on a NPRM must be reviewed by the agency and the agency must respond to these comments in a subsequent Federal Register notice before issuing the final rule. The rulemaking process is used to allow individuals and organizations to comment on such collections before an agency may issue these rules and notices as final.

Generally speaking, under the statutes that created the Chief Privacy Officer and Civil Liberties Protection Officer in the Office of the Director of National Intelligence, each officer is responsible for reviewing and approving all Privacy Impact Assessments (PIAs), a requirement under one of the three pillars of federal privacy law, Section 208 of the E-Government Act. A PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. PIAs are posted on a federal agency's website[13] and published in the Federal Register.[14] Indeed, PIAs must be published in order to receive funding by OMB.[15]

c. Redress and Inquiry through the Privacy Pillars

Two of the pillars of federal privacy law mandate government transparency to individuals about whom it has collected and maintains information. The FOIA provides any person, regardless of citizenship or location, an administrative process to seek access to information about them.[16] Closely associated with this is the Privacy Act that requires agencies to have an administrative process to allow U.S. citizens or lawful permanent residents to seek access and amendment to records about them, subject to certain exemptions.[17]

d. Administrative Processes and Policy Commitments

While the Privacy Act does not grant rights of amendment to non-U.S. persons,[18] some agencies have established an administrative process apart from the procedures provided by the Privacy Act that allows non-U.S. persons the opportunity for redress of information concerning them. For example, the DHS Traveler Redress Inquiry Program (TRIP) allows any individual – regardless of nationality – to seek redress for the records maintained by DHS components responsible for transportation and border security.

While not legally binding, privacy policy commitments made by the head of an agency are carried out and enforced by senior agency officials. For instance, in the case of DHS, Secretary Chertoff has urged the Privacy Office to apply strong privacy protections for all persons included in DHS systems, regardless of citizenship. 'If we want to protect the privacy of our own citizens, we are going to have to be willing to protect the privacy of our international partners and their citizens. And that means we have to protect shared information and continue to demonstrate a level of trust … I trust that the Privacy Office will be equally vigorous in insuring that American data is protected in the E.U. to the same or a higher degree.'[19] The DHS CPO issued a department-wide policy to afford privacy protections for non-U.S. persons in DHS systems of records.[20]

e. National Archives and Records Administration or the Archivist

The Archivist, appointed by the President without regard to political affiliation and confirmed by the Senate, is authorised by law to "inspect the records or the records management practices and programs of any Federal agency" for the purpose of making recommendations for improving records management practices and programs. Key among his responsibilities is the Federal Records Act, which provides for records retention schedules and penalties for the improper destruction or alienation of federal records. Agencies are also required to obtain approval of the Archivist for retention schedules and follow its guidance for deletion. Privacy records also fall within the purview of the Archivist. The Archivist should be considered part of the extended federal privacy network.

f. Inspectors General

Every large U.S. government agency, including DHS and DOJ, has an Inspector General. Widely recognized throughout the federal government as independent, inspectors general at cabinet level agencies (*e.g.*, DHS, DOJ, Treasury, and Defense) are appointed by the Senate with the advice and consent of the Senate and at certain designated federal entities they are appointed by the head of the agency.[21] They are subject to the general supervision of the agency head, and if fired, the agency head must inform Congress of the removal. Inspectors General are authorized by law to conduct independent investigations, audits, inspections and special reviews of individual actions and programs to detect and deter waste, fraud, abuse and misconduct. In addition to required bi-annual reports to Congress, Congress may require that the Inspector General provide specialized reports or the Inspector General may independently determine to initiate an investigation. Such investigations may include privacy related issues. For example, the Department of Justice Inspector General recently issued a report to Congress on the FBI's use of National Security Letters.[22] The Department of Homeland Security Inspector General concluded an investigation into DHS's handling of Personally Identifiable Information.[23] The process is transparent with IG reports publicly available. Inspectors General often work with the Privacy Offices at DHS, DOJ and DNI to assist with their oversight functions. Given their independent standing, IG's fall outside the privacy network and are best understood as an additional layer of oversight.

g. Federal Employee Rights and Protections

Often forgotten, but an effective oversight tool nevertheless, are the rights and protections afforded federal employees. The First Amendment to the Constitution guarantees every citizen's rights of free speech and to petition Congress.

Closely tied to this Constitutional right, are the protections afforded federal employees under the Whistleblower Protection Act (WPA), which provides an additional layer of oversight. Federal employees who engage in "whistleblowing," that is, making a disclosure indicating illegal or improper government activities, are protected from retaliatory treatment at the agency.[24] This could include disclosures to supervisors, inspectors general, Congress, or even the media. The protections of the WPA apply to most federal executive branch employees and become applicable when a personnel action is taken because of a "protected disclosure" made by an employee. The WPA is relevant to the privacy oversight framework where a federal employee may make a disclosure concerning the improper use of privacy information. The independent Office of Special Counsel oversees the Whistleblower Act and can bring actions against an agency or its officers and employees who have committed prohibited personnel practices in addition to investigating allegations of retaliatory behavior.

B. Congress

Within the separation of powers among the three co-equal branches of the federal government, Congress holds the "power of the purse." No monies may be spent by the Executive Branch without authorization and appropriation by Congress. Through the authorization and appropriations process, Congress instructs the executive branch on what it can and cannot do with the funds Congress provides. Congress is one of the layers of oversight and accountability.

1. Congressional Committees

Critical to it fiscal responsibility to the American People, is Congress's oversight of the executive branch activities through its committees. Congress could issue reports and withhold funding based on negative findings in an investigation of an agency's handling of personal information.

The frequency and level of hearings and the level of detail they may cover can be extensive. For example, in 2006, DHS officials testified at 206 hearings, conducted approximately 2,242 congressional briefings and received more than 2,000 post Hearing Questions for the Record (QFRs). Many hearings and QFRs touched on privacy directly or indirectly.

2. The Government Accountability Office (GAO)

The GAO, which is independent and nonpartisan, is Congress' investigative arm. At Congressional request, the GAO investigates audits and evaluates executive branch agencies and the programs and expenditures of the federal government. The GAO is created by statute, which specifically defines its powers to conduct reviews and investigations and issue legal opinions. When GAO reports its findings to Congress and the heads of executive departments and agencies, it recommends actions. It has issued numerous reports analysing agencies' handling of personal information specifically addressing law enforcement and national security.[25] For example, the GAO conducted extensive investigations and reported on privacy protections and compliance in a DHS aviation security system called Secure Flight.[26] Its final recommendations to DHS included taking several actions to manage risks associated with Secure Flight's

development, such as finalizing privacy and redress requirements. In early 2007, the GAO completed reviews and reports on health information technology[27] and data privacy, improvements to FOIA,[28] and the DHS Privacy Office.[29]

C. Judiciary

Two of the three pillars of federal privacy law provide for legal redress. The Privacy Act provides for four separate and distinct civil causes of action – two of which are injunctive (amendment and access) and two of which provide for monetary damages (accuracy lawsuits and lawsuits for other damages).[30] The limitation, however, is that only U.S. persons legal permanent residents are granted standing in the courts to pursue claims under the Privacy Act. Non-U.S. persons may seek amendment of their records through administrative programs established outside the procedures afforded by the Privacy Act like the DHS Traveler Redress and Inquiry Program, however. The Judiciary is one more layer of oversight and accountability.

Under the FOIA, any person may challenge an agency's response to his or her FOIA request in federal court. Access to the court system is permitted regardless of citizenship or resident status. Agencies must comply with court orders regarding access to records. FOIA requestors who prevail in court may even be entitled to attorney's fees and litigation costs. While FOIA does not provide any award of monetary damages to a requester, the Act does provide in certain limited circumstances (where agency employees who have acted arbitrarily and capriciously) to withhold information may be subject to disciplinary action.

D. The Public Privacy Community

The executive branch, Congress and the judiciary are the formal actors under the Constitution. There are also other less formal but still influential oversight mechanisms. The U.S. enjoys a large and active advocacy community consisting of non-governmental organizations dedicated to privacy and related civil liberties. These groups are accepted as part of the democratic process and serve as vigorous public watchdogs. Agencies frequently seek their input through written and oral consultations. During the notice and comment period of privacy regulations, comments from the advocacy community are often the most informed.

II. Recognition of U.S. Oversight Internationally

The U.S. is party to a number of agreements and arrangements in the law enforcement public and national security area where U.S. privacy oversight and accountability have been recognized internationally. As a Member of the European Parliament and Rapporteur of the Committee on Civil Liberties, Justice and Home Affairs, Sophie In´t Veld, recently commented, "the US has much stricter privacy rules than Europe, and they are much better at democratic oversight and self-criticism."[31]

In the past five years, European Union institutions and member states have repeatedly demonstrated confidence in the United States' ability to protect personally identifiable information exchanged for law enforcement and public safety purposes. This respect for the U.S.' handling of personal data and respect for its mechanisms for maintaining accountability has been demonstrated through execution of several binding international agreements. In December 2001, the United States and Europol signed a cooperation agreement, and in

December 2002 a supplemental agreement for the sharing of personally identifiable information. In November 2006, the U.S. and Eurojust concluded a cooperation agreement for the sharing of personally identifiable information. Article 12 of the 2002 Europol supplemental agreement provides that the United States shall conduct oversight of its implementation in accordance with applicable law and procedures, utilizing administrative, judicial or supervisory bodies that ensure an appropriate level of independence. Article 19 of the 2006 Eurojust agreement contains a similarly-worded provision. The Europol and Eurojust Agreements were approved by those institutions' data protection supervisory authorities, and in effect serve as formal determinations that conditions for sharing information with the United States have been met.

In addition, in June 2003, the United States and the European Union concluded agreements on Mutual Legal Assistance and Extradition. Subsequently, all 25 member states (before the January 2007 enlargement) concluded bilateral instruments with the United States implementing these agreements. Among the provisions in the Mutual Legal Assistance agreement is an article governing the use of personal data in the context of criminal investigations and prosecutions, related administrative proceedings, and for preventing imminent and serious threats to public security. This provision, drawn from the U.S.-Germany Mutual Legal Assistance Treaty, both insures prosecutors the flexibility they need and protects personal data in line with the requirements of European legislation.

In reviewing the US-E.U. PNR Agreement and Undertakings, the E.U. Advocate General in the PNR cases observed that, "The Chief Privacy Officer is not a judicial authority. However…the Officer is an administrative authority with some degree of independence from the Department of Homeland Security."[32] The Advocate General went on to find that allowing "airline passengers to lodge a complaint with the Chief Privacy Officer and the availability to them of a judicial remedy under the FOIA constitute significant safeguards with regard to their right to respect for their private life."[33]

Implicit in this is the E.U. acceptance that the U.S. framework provides acceptable powers of accountability and oversight over personally identifiable information. Since the U.S. and E.U. have different systems of government, this language allowed for mutual recognition of our varying systems.
6
Outside of the E.U., the U.S. and Canada negotiated an agreement to share asylum data. In this case, both systematic and case-by-case sharing of asylum information between Canada and the U.S. is allowed under a formal arrangement known as the Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims (the "Annex"), which falls under an umbrella agreement, the Statement of Mutual Understanding on Information Sharing between Canada and the U.S. Before signing the Annex, U.S. and Canadian governments carefully considered each other's confidentiality and privacy rules and practices to gain assurance that shared information would be protected appropriately. The privacy and confidentiality rules of each country also required that certain steps be taken at high-levels of the government before implementing the information-sharing arrangement. The Canadian government performed a Privacy Impact Assessment in order to demonstrate that the sharing of asylum information under the Annex would not unduly affect the asylum applicants' privacy rights. The Privacy Impact Assessment was reviewed and approved by Canada's Privacy Commissioner.

Additionally, the Department of State and DHS entered into personal information sharing commitments with Australia and New Zealand to protect privacy of individuals in an MOU[34] to share lost and stolen passport information. By signing the MOU, each party explicitly recognized the other party's high level of oversight and enforcement of data protection provisions related to the information being exchanged.[35]

Finally, while outside the scope of traditional criminal law enforcement and home affairs, it is worth nothing that U.S. independent agencies share confidential personally identifiable information with foreign law enforcers for purposes of investigating or pursuing fraud, reception, spam, spyware and other commercial violations.[36] Such investigations can later be referred to the Attorney General for prosecution. These exchanges are further international recognition of the effective oversight and accountability of U.S. agencies over personally identifiable information.

III. CONCLUSION

Oversight and accountability in the U.S. Government are organic to the U.S. Constitution and our democratic form of government. While complex, the Constitutional authorities of the Congress, the executive branch and the judiciary are transparent, open and responsive to the demands of individuals.

---

[1] John W. Kropf is the Director of International Privacy Policy for the Department of Homeland Security's Privacy Office. The views expressed here are his and not those of the Department of Homeland Security or the U.S. Government. The author wishes to acknowledge contributions from colleagues at DHS, Department of Justice and the Department of State with special recognition for DHS International Privacy Analysts, Shannon Ballard and Lauren Saadat.

[2] The 9/11 Commission Report, page 390

[3] For example, a new mechanism to replace the temporary U.S.-E.U. PNR Agreement due to expire July 2007.

[4] Regulations are rules and administrative codes issued by governmental agencies at all levels, municipal, county, state and federal. Although they are not laws, regulations have the force of law, since they are adopted under authority granted by statutes, and often include penalties for violations.

[5] Executive Orders are a Presidents or Governors declaration which has the force of law, usually based on existing statutory powers, and requiring no action by the Congress or state legislature.

[6] A policy is a plan of action to guide decisions and actions.

[7] An executive agency that intends to adopt a rule must give public notice of its intention in the *Federal Register.* The published notice, called a Notice of Proposed Rulemaking (or NPRM), typically requests public comment on a proposed rule, and provides notice of any public meetings where a proposed rule will be discussed. The public comments are considered by the issuing government agency, and the text of a final rule is published in the *Federal Register*.

[8] For a complete set of privacy guidance directives issued by OMB, see their website at: *www.whitehouse.gov/omb/privacy/*.

[9] Homeland Security Act of 2003, section 222(f).

[10] www.privacyboard.gov/

[11] The Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. No. 109-162).

[12] The Consolidated Appropriations Act, Fiscal Year 2005 (Pub. L. No. 108-447).

[13] See for example, *www.dhs.gov/privacy*

[14] The Federal Register is also available on the world wide web. See *www.gpoaccess.gov/fr/*

[15] See OMB M-03-22 Memorandum, www.whitehouse.gov/omb/memoranda/m03-22.html

[16] For example, in 2005 the Department of Justice processed 51,435 FOIA requests. That same year, the Department of Homeland Security processed 126,126 requests. Of those, DHS received 37 FOIA requests from 17 countries.

[17] See DHS Privacy Office website at *www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf*
[18] For ease of reference, this article will refer to those covered by the Privacy Act as ''U.S. persons'' and those not covered as ''non-U.S. persons.'' The Privacy Act applies to ''a citizen of the United States or an alien lawfully admitted for permanent residence.'' 552a(a)(2).
[19] DHS Secretary Michael Chertoff, prepared remarks delivered to the DHS Privacy Advisory Committee, December 6, 2005.
[20] Policy statement can be found at *www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf*.
[21] For a recent discussion of Inspectors General, see *Government Oversight – The Watchdogs*, Peter H. Stone, National Journal, May 12, 2007.
[22] www.usdoj.gov/oig/
[23] *www.dhs.gov/xoig/assets/mgmtrpts/OIGr_07-24_Jan07.pdf*
[24] 24 5 U.S.C. 1201
[25] For GAO reports on law enforcement and homeland security information systems as well as numerous other topics, see *www.gao.gov/*
[26] *www.gao.gov/new.items/d05356.pdf*
[27] *www.gao.gov/new.items/d07400t.pdf*
[28] *www.gao.gov/new.items/d07491t.pdf*
[29] *www.gao.gov/docsearch/abstract.php?rptno=GAO-07-52230*
[30] See 5 U.S.C. 552a(g).
[31] *www.neurope.eu/view_news.php?id=71636*
[32] Opinion of the EU Advocate General, Cases C-317/04 and C-318/04, November 22, 2005, paragraph 252.
[33] Id at 253.
[34] *www.apec.org/apec/documents_reports/informal_experts_group_business_mobility/2006.html*
[35] For a discussion of the privacy of non-U.S. persons in the context of international agreements, see Kropf, The Privacy of Foreign Nationals, BNA Privacy and Security Law Report, Vol. 3, No. 46. At 1306 (November 15, 2004).
[36] For example, the Federal Trade Commission (FTC) has entered into bilateral cooperation agreements with agencies in Australia, Canada, Ireland, Mexico, and the United Kingdom and executed memoranda of understanding on spam enforcement with agencies in Australia, the United Kingdom, and Spain.